Abstract

The present invention provides a method of authenticating a pair of correspondents in a communication system, such as in a mobile phone network by utilizing a blend of public-key cryptography and symmetric cryptography. Each session between the mobile phone and the network consists of public-key based mutual authentication and key exchange followed by symmetric-key secure data exchange.